ỦY BAN NHÂN DÂN XÃ PHƯỚC GIANG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 1652/QĐ-UBND	*Phước Giang, ngày 14 tháng 8 năm 2026*

QUYẾT ĐỊNH
Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng đối với Hệ thống thông tin Đảng ủy, HĐND, UBND xã Phước Giang

ỦY BAN NHÂN DÂN XÃ PHƯỚC GIANG

Căn cứ Luật Tổ chức chính quyền địa phương ngày 16/6/2025;

Căn cứ Luật An ninh mạng ngày 10/12/2025;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Chỉ thị số 09/CT-TTg ngày 23/02/2024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông về quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Theo đề nghị của Trưởng phòng Văn hóa – Xã hội.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế bảo đảm an toàn, an ninh mạng đối với Hệ thống thông tin Đảng ủy, HĐND, UBND xã Phước Giang".

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 3. Chánh Văn phòng HĐND và UBND, Trưởng phòng Văn hóa – Xã hội; Thủ trưởng các cơ quan, đơn vị và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành quyết định này./.

Nơi nhận:
- Như Điều 3;
- Thường trực Đảng ủy;
- Thường trực HĐND xã;
- CT, các PCT UBND xã;
- VP HĐND&UBND;
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

U.B.N.D XÃ PHƯỚC GIANG T. QUẢNG NGÃI

Nguyễn Văn Lễ

ỦY BAN NHÂN DÂN **XÃ PHƯỚC GIANG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**

QUY CHẾ
Bảo đảm an toàn, an ninh mạng đối với Hệ thống thông tin Đảng ủy, HĐND, UBND xã Phước Giang

(Kèm theo Quyết định số 1652/QĐ-UBND ngày 14 tháng 8 năm 2026 của Ủy ban nhân dân xã Phước Giang)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Phạm vi điều chỉnh

Quy chế này quy định các chính sách quản lý và các biện pháp nhằm bảo đảm an toàn, an ninh mạng đối với Hệ thống thông tin Đảng ủy, HĐND, UBND xã Phước Giang, bao gồm:

- Phạm vi quản lý về vật lý và logic của tổ chức;

- Các ứng dụng, dịch vụ hệ thống cung cấp;

- Nguồn nhân lực bảo đảm an toàn thông tin.

2. Đối tượng áp dụng

a) Các đơn vị thuộc Đảng ủy, HĐND, UBND xã Phước Giang; cán bộ thuộc các đơn vị thuộc Đảng ủy, HĐND, UBND xã Phước Giang.

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng hệ thống thông tin Đảng ủy, HĐND, UBND xã Phước Giang.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển và bảo đảm an toàn thông tin mạng phục vụ hoạt động của hệ thống thông tin Đảng ủy, HĐND, UBND xã Phước Giang.

Điều 2. Giải thích từ ngữ

Trong quy chế này, các từ ngữ dưới đây được hiểu như sau:

An toàn thông tin mạng: Là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

Mạng: Là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

Hệ thống thông tin: Là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

Chủ quản hệ thống thông tin: Là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

Điều 3. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin

1. Mục tiêu bảo đảm an toàn thông tin

Bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin Hệ thống thông tin Đảng ủy, HĐND, UBND xã Phước Giang.

2. Nguyên tắc

a) Cơ quan, tổ chức thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn, an ninh mạng đối với Hệ thống thông tin Đảng ủy, HĐND, UBND xã Phước Giang theo quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền và các quy định tại Quy chế này.

b) Bảo đảm an toàn thông tin (ATTT) là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình:

- Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu.

- Thiết kế, thiết lập và vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

c) Việc bảo đảm an toàn thông tin hệ thống thông tin được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

Điều 4. Những hành vi nghiêm cấm

Các hành vi bị nghiêm cấm về an ninh mạng quy định tại Điều 7 Luật An ninh mạng:

1. Đăng tải, phát tán thông tin có nội dung sau trên không gian mạng:

a) Tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm: tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân; chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước; xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc;

b) Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc;

c) Bịa đặt, vu khống, thông tin sai sự thật, xâm phạm nhân phẩm, danh dự, uy tín của người khác hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;

d) Sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động bình thường của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác; thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền,

trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác; thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, kinh doanh theo phương thức đa cấp, chứng khoán.

2. Thực hiện hành vi sau trên không gian mạng:

a) Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam;

b) Kích động, kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân; kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự;

c) Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh; chiếm đoạt, mua bán, thu giữ, cố ý làm lộ bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; cố ý nghe lén, ghi âm, ghi hình trái phép các cuộc đàm thoại trên không gian mạng; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc;

d) Hoạt động mại dâm, tệ nạn xã hội, mua bán người, các bộ phận cơ thể người; tuyên truyền văn hóa phẩm dâm ô, đồi trụy; kích động, cổ xúy bạo lực, lối sống trụy lạc, lệch chuẩn, phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng;

đ) Lừa đảo chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng;

e) Giả mạo trang thông tin điện tử của cơ quan, tổ chức, cá nhân; làm giả, lưu hành, trộm cắp, mua bán, thu thập, trao đổi trái phép thông tin thẻ tín dụng, tài khoản ngân hàng, tài sản mã hóa, tài sản số của người khác; phát hành, cung cấp, sử dụng trái phép các phương tiện thanh toán; giả mạo giấy tờ của cơ quan, tổ chức;

g) Sử dụng trí tuệ nhân tạo hoặc công nghệ mới để giả mạo video, hình ảnh, giọng nói của người khác trái quy định của pháp luật; tạo lập, đăng tải, phát tán thông tin quy định tại khoản 1 Điều này;

h) Thu thập, sử dụng, phát tán, trao đổi, chuyển nhượng, kinh doanh trái pháp luật thông tin, dữ liệu cá nhân của người khác;

i) Hướng dẫn, xúi giục, lôi kéo, kích động người khác phạm tội hoặc thực hiện hành vi vi phạm pháp luật;

k) Thực hiện hành vi khác trên không gian mạng bằng việc sử dụng công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội.

3. Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng, tội phạm sử dụng công nghệ cao; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin.

4. Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoặc phát tán thư rác, tin nhắn rác, cuộc gọi rác, chương trình tin học gây hại đến hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử.

5. Xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác.

6. Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng.

7. Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi.

8. Hành vi khác vi phạm quy định của Luật này.

Điều 5. Phối hợp với những cơ quan/tổ chức có thẩm quyền

1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin: UBND xã Phước Giang giao Phòng Văn hóa – Xã hội là đầu mối liên hệ, phối hợp các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho hệ thống thông tin của mình.

Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin:

a) Công an tỉnh (Thường trực Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao)

+ Người liên hệ/bộ phận: Tiểu ban An toàn, an ninh mạng

+ Số điện thoại 24/7: 0694.309.485 hoặc 0888.309.485

+ Email: tieubanatanm@quangngai.gov.vn

+ Địa chỉ: 403 Lê Lợi, Nghĩa Lộ, Quảng Ngãi.

b) Bộ Công an/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam

Người liên hệ/bộ phận: Ban Giám sát và ứng cứu sự cố

Số điện thoại 24/7: 0692205199

Email: report@vncert.vn

Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: soar.soc.gov

3. Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

UBND xã hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

Điều 6. Bảo đảm nguồn nhân lực

1. Tuyển dụng

Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

2. Trong quá trình làm việc

a) Quy định về việc thực bảo đảm an toàn thông tin trong quá trình làm việc:

- Cán bộ chuyên trách phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển trung cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin.

- Cán bộ chuyên trách phải tổ chức quản lý định doanh đối với tất cả người sử dụng tham gia gia sử dụng hệ thống thông tin.

- Các bộ phận, cá nhân tham gia sử dụng dịch vụ của hệ thống phải tuân thủ các quy định về bảo đảm an toàn, an ninh mạng và chịu trách nhiệm đối với mọi hoạt động trên tài khoản truy cập của mình đã được cấp.

- Tài khoản quản trị hệ thống (mạng, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu…) phải tách biệt với tài khoản truy cập của người sử dụng thông thường. Tài khoản quản trị hệ thống phải giao đích danh cá nhân làm quản công tác quản trị. Phân quyền sử dụng tài khoản quản trị theo chức năng nhiệm vụ của cá nhân trong công tác vận hành quản trị hệ thống.

b) Với người sử dụng:

- Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc. Trước khi tham gia vào hệ thống phải được kiểm tra khả năng đáp ứng các yêu cầu về ATTT.

- Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT.

- Chỉ truy cập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp chức năng, trách nhiệm, quyền hạn của mình; không truy cập, mở các trang tin, thư điện tử không rõ nguồn gốc.

- Có trách nhiệm bảo mật tài khoản truy cập thông tin, không chia sẻ mật khẩu với người khác. Đặt mật khẩu với an toàn cao và thay đổi mật khẩu tối thiểu 01 lần/tháng; các tài khoản đăng nhập các hệ thống phải được đăng xuất khi không sử dụng. Thực hiện các biện pháp mã hóa đối với các tài khoản, mật khẩu được lưu trên thiết bị.

- Khóa máy tính khi tạm thời rời nơi đặt máy tính; tắt máy tính khi rời khỏi cơ quan.

- Phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.

c) Định kỳ hàng năm tổ chức hoặc tham gia phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng do đơn vị chức năng tổ chức.

3. Chấm dứt hoặc thay đổi công việc

a) Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức.

b) Bộ phận chuyên trách thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

Điều 7. Bảo đảm an ninh mạng, an toàn thông tin khi sử dụng máy tính và thiết bị ngoại vi

1. Máy tính và thiết bị ngoại vi của đơn vị phải được cài đặt hệ điều hành, phần mềm soạn thảo văn bản, phần mềm chuyên dụng để xử lý công việc và tuân thủ các quy định sau:

a) Chỉ cài đặt phần mềm hợp lệ (phần mềm có bản quyền thương mại, phần mềm nội bộ hoặc phần mềm mã nguồn mở được đầu tư (hoặc thuê dịch vụ) có nguồn gốc rõ ràng) và thuộc danh mục phần mềm được phép sử dụng do đơn vị có thẩm quyền của UBND tỉnh ban hành (nếu có); không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin thường xuyên cập nhật phần mềm và hệ điều hành.

b) Cài đặt phần mềm xử lý phần mềm độc hại và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; thực hiện kiểm tra, rà quét phần mềm độc hại khi sao chép, mở các tập tin hoặc trước khi kết nối các thiết bị lưu trữ dữ liệu di động với máy tính của mình.

c) Khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính (máy chạy chậm bất thường, báo lỗi phần mềm, cảnh báo chống phần mềm độc hại, mất dữ liệu...), phải tắt máy và báo trực tiếp cho cơ quan, bộ phận chuyên trách về công nghệ thông tin để được xử lý kịp thời.

d) Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; sử dụng những trình duyệt an toàn; không truy nhập, mở các trang tin, thư

điện tử không rõ nguồn gốc; không sử dụng tính năng lưu mật khẩu tự động hoặc đăng nhập tự động.

đ) Có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác. Đặt mật khẩu với độ an toàn cao (tối thiểu 8 ký tự bao gồm: có chữ thường, có chữ in hoa, có số và ký tự đặc biệt như @, #, ! ...), và thay đổi mật khẩu tối thiểu 6 tháng/lần; các tài khoản đang nhập các hệ thống phải được đăng xuất khi không sử dụng; thường xuyên xóa bộ nhớ cache và cookie trong trình duyệt trên máy tính.

e) Thực hiện thao tác khóa máy tính (sử dụng tính năng có sẵn trên máy tính) khi rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi đơn vị.

2. Trước khi mang máy tính, thiết bị có cổng mạng thông tin có kết nối mạng nội bộ ra ngoài đơn vị làm việc và kết nối với mạng nội bộ để thực hiện xử lý công việc phải báo cáo và phải được lãnh đạo đơn vị đồng ý, cho phép. Trong trường hợp này, cá nhân phải tuân thủ đầy đủ các quy định tại các điểm a, b, c, d, đ, e khoản 1 Điều này và chịu sự giám sát của bộ phận chuyên trách về công nghệ thông tin của đơn vị.

3. Đối với thiết bị soạn thảo, lưu trữ bí mật nhà nước:

a) Các đơn vị phải bố trí ít nhất một máy tính độc lập, máy in (photocopy) không kết nối và không có lịch sử kết nối với mạng Internet, mạng máy tính, mạng viễn thông, trừ trường hợp lưu giữ bí mật nhà nước theo quy định của pháp luật về cơ yếu để soạn thảo, lưu trữ các văn bản có nội dung bí mật nhà nước.

b) Công chức, viên chức, nhân viên được giao nhiệm vụ trong quá trình xử lý công việc, soạn thảo văn bản có nội dung BMNN chỉ sử dụng máy tính, thiết bị riêng biệt, bảo đảm các yêu cầu của pháp luật về bảo vệ bí mật nhà nước và cơ yếu.

Chương II
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ THIẾT KẾ, XÂY DỰNG HỆ THỐNG

Điều 8. Đảm bảo an toàn thông tin

a) Hệ thống mạng phải được thiết kế thống nhất, được quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý và bảo đảm an toàn và bảo mật.

b) Hệ thống thông tin phải được bảo vệ bằng tường lửa (có thể tích hợp tường lửa trên modem hoặc router) và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng.

c) Mạng không dây (WI-FI), cần thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn.

d) Phải kiểm tra hoạt động tổng thể của hệ thống sau khi thay đổi cấu hình hoặc nâng cấp hệ thống.

e) Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố:

- Định kỳ hàng tháng hoặc khi có thay đổi, bộ phận chuyên trách thực hiện sao lưu, dự phòng hệ thống trên hệ thống độc lập như USB, DVD, SAN hoặc lưu trữ trên hạ tầng đám mây (cloud).

- Các dữ liệu sau yêu cầu sao lưu, dự phòng: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

g) Truy cập và quản lý cấu hình hệ thống:

- Cấu hình hệ thống từ xa phải sử dụng các giao thức bảo mật có mã hóa thông tin như SSL, TSL, SSH, VPN.

- Khi cấu hình hệ thống từ bên ngoài phải thông qua kết nối VPN.

- Toàn bộ cấu hình hệ thống phải được lưu trên thiết bị hoặc hệ thống lưu trữ độc lập.

Điều 9. Thiết kế an toàn hệ thống thông tin

1. Đơn vị thiết kế, xây dựng HTTT phải cung cấp tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành HTTT:

- Tài liệu phân tích lựa chọn kiến trúc, công nghệ;

- Tài liệu thiết kế tổng thể hệ thống thể hiện thiết kế hạ tầng và kết nối các thành phần của hệ thống;

- Các giải pháp, thiết bị của HTTT đáp ứng các quy định của Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn HTTT theo cấp độ (Thông tư số 12/2022/TT-BTTTT).

2. Đơn vị thiết kế, xây dựng HTTT phải cung cấp các tài liệu "Kiến trúc hệ thống" trong đó có mô tả thiết kế và các thành phần của HTTT thông qua một số mô hình kiến trúc khác nhau nhằm miêu tả hệ thống dưới nhiều góc nhìn khác nhau, bao gồm:

- Thiết kế kiến trúc ứng dụng;

- Thiết kế kiến trúc dữ liệu;

- Thiết kế kiến trúc vật lý.

3. Đơn vị thiết kế, xây dựng HTTT phải cung cấp tài liệu mô tả phương án bảo đảm ATTT theo cấp độ được quy định tại Thông tư số 12/2022/TT-BTTTT.

4. Đơn vị thiết kế, xây dựng HTTT phải cung cấp tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm ATTT, trong đó cần đảm bảo các tiêu chí:

- Đảm bảo có từ 2 - 3 công nghệ được phân tích và đưa ra phương án lựa chọn;

- Phân tích các ưu, nhược điểm của từng công nghệ để từ đó chọn ra công nghệ áp dụng phù hợp nhất.

5. Khi có thay đổi thiết kế, cần đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

Khi có thay đổi thiết kế, đơn vị thiết kế, xây dựng HTTT, cần phối hợp với các đơn vị liên quan đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống, xây dựng kế hoạch trước khi có thay đổi, kèm theo các tài liệu sau:

- Căn cứ thực hiện thay đổi (công văn, tờ trình);

- Kế hoạch chi tiết các bước thực hiện.

6. Phương án quản lý và bảo vệ hồ sơ thiết kế

Hồ sơ thiết kế được sắp xếp một cách khoa học để dễ quản lý, dễ nộp lưu và dễ tìm khi cần. Hồ sơ thiết kế được giữ gìn bí mật, bảo quản theo chế độ tài liệu mật, không được mang hồ sơ thiết kế ra khỏi cơ quan hoặc tùy tiện cung cấp hồ sơ thiết kế cho cá nhân, đơn vị khác.

Điều 10. Phát triển phần mềm thuê khoán

1. Đối với các nội dung liên quan đến việc phát triển phần mềm, đơn vị được thuê khoán phải đảm bảo có các tài liệu sau:

- Biên bản làm việc.

- Biên bản thống nhất nội dung công việc.

- Hợp đồng giữa các đơn vị.

- Hồ sơ liên quan đến ATTT, bảo mật của phần mềm, cơ sở dữ liệu; các cam kết đảm bảo ATTT, an ninh mạng.

2. Nhà phát triển phần mềm phải cung cấp mã nguồn sản phẩm cho đơn vị xây dựng phần mềm theo hình thức ghi đĩa DVD hoặc USB; yêu cầu tệp trên DVD, USB cần phải đặt mật khẩu để đảm bảo ATTT

- Mã nguồn đã được nhà phát triển tự đánh giá và có biên bản kiểm thử, đánh giá Đạt trước khi bàn giao cho đơn vị thuê.

- Phối hợp với đơn vị chủ quản HTTT đánh giá mã nguồn và có phương án xử lý lỗi (nếu có).

3. Kiểm thử phần mềm trên môi trường thử nghiệm và nghiệm thu trước khi đưa vào sử dụng

Đơn vị thuê và đơn vị phát triển phối hợp thực hiện kiểm thử phần mềm trên môi trường thử nghiệm và nghiệm thu trước khi đưa vào sử dụng:

- Mã nguồn phải được đánh giá ATTT trước khi đưa vào môi trường thử nghiệm và nghiệm thu trước khi đưa vào sử dụng.

- Tất cả các lỗi liên quan đến mã nguồn (nếu có) sau khi được khắc phục, phải được đánh giá ATTT và có biên bản đánh giá trước khi đưa vào sử dụng.

4. Kiểm tra, đánh giá ATTT, trước khi đưa vào sử dụng

Hệ thống được đầu tư phải được kiểm định ATTT trước khi đưa vào vận hành khai thác:

- Kiểm tra hệ thống, mã nguồn có các lỗ hổng bảo mật không. Thực hiện cập nhật các bản vá ATTT hoặc nâng cấp lên phiên bản mới nhất của hãng để đảm bảo vá hoàn toàn các lỗ hổng bảo mật.

- Thực hiện nâng cấp, xử lý điểm yếu ATTT của thiết bị hệ thống trước khi đưa vào sử dụng.

- Máy chủ phải được cài đặt hệ điều hành, phần mềm, phần mềm diệt virus có bản quyền.

5. Kiểm tra, đánh giá ATTT cho phần mềm khi thay đổi mã nguồn, kiến trúc phần mềm

Khi có thay đổi thiết kế, đơn vị thuê và đơn vị phát triển phần mềm phối hợp đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống, cần xây dựng kế hoạch trước khi có thay đổi bao gồm tối thiểu các tài liệu sau:

- Căn cứ thực hiện thay đổi (công văn, tờ trình);

- Kế hoạch chi tiết các bước thực hiện.

6. Cam kết đảm bảo tính bí mật của mã nguồn và bản quyền của phần mềm phát triển:

- Bên phát triển phải có cam kết về bảo đảm tính bí mật của mã nguồn, không cung cấp cho tổ chức hoặc cá nhân khác.

- Bên phát triển có cam kết không có tranh chấp về bản quyền phát triển của phần mềm.

- Các cá nhân tham gia phát triển, triển khai HTTT phải ký biên bản cam kết bảo mật ATTT.

Điều 11. Thử nghiệm và nghiệm thu hệ thống

1. Thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng.

Các sản phẩm, thiết bị được đầu tư trong hệ thống phải được kiểm định ATTT trước khi đưa vào vận hành khai thác:

- Kiểm tra phiên bản phần mềm cho phần cứng (firmware) các thiết bị mạng quan trọng như: Tường lửa, Switch, IDS/IPS,... có lỗ hổng bảo mật không. Thực hiện cập nhật các bản vá hoặc nâng cấp lên phiên bản mới nhất của hãng để đảm bảo ATTT.

- Các thiết bị hệ thống trước khi được đưa vào sử dụng phải được qua kiểm định về an ninh, an toàn, cháy nổ theo quy định của các cơ quan chức năng; thực hiện nâng cấp, xử lý điểm yếu ATTT trước khi đưa vào sử dụng.

- Đảm bảo máy chủ không chứa mã độc; thực hiện gỡ bỏ các hệ điều hành cũ đối với máy chủ và thực hiện xóa dữ liệu (Format) đối với các ổ cứng trước khi đưa vào sử dụng.

2. Nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống.

a) Hệ thống được thử nghiệm tổng thể trước khi đưa vào sử dụng và định kỳ hàng năm để đảm bảo tính an toàn, thống nhất của hệ thống.

b) Nội dung, kế hoạch và quy trình nghiệm thu hệ thống được thực hiện theo Thông tư số 24/2020/TT-BTTTT ngày 09/9/2020 của Bộ Thông tin và Truyền thông quy định về công tác triển khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng CNTT sử dụng nguồn vốn ngân sách nhà nước.

c) Quy trình thử nghiệm và nghiệm thu hệ thống theo Phụ lục II.

3. Cơ quan có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống

Đơn vị vận hành đảm nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống như sau:

- Kiểm thử, nghiệm thu chức năng của hệ thống.

- Kiểm thử, nghiệm thu bảo đảm ATTT.

- Kiểm thử, nghiệm thu hệ thống nội bộ của đơn vị phát triển.

4. Đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống.

5. Báo cáo nghiệm thu được ký xác nhận của Ủy ban nhân dân xã Phước Giang trước khi đưa vào sử dụng.

Chương III
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ VẬN HÀNH HỆ THỐNG

Điều 12. Quản lý an toàn mạng

1. Quản lý, vận hành hoạt động bình thường của hệ thống

a) Thực hiện việc quản lý và kiểm soát mạng nhằm ngăn ngừa các nguy cơ, rủi ro và duy trì an toàn cho các máy tính, ứng dụng sử dụng mạng:

- Có sở đồ logic và vật lý về hệ thống mạng, tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn và bảo mật.

- Sử dụng thiết bị tường lửa, thiết bị phát hiện và kiểm soát truy từ bên ngoài mạng và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng; Kiểm soát truy cập từ bên trong mạng; kết nối hệ thống giám sát tập trung (nếu có); Phòng chống xâm nhập giữa các vùng mạng; Phòng chống phần mềm độc hại trên môi trường mạng.

b) Thiết lập, cấu hình đầy đủ các tính năng của thiết bị mạng. Thường xuyên, kiểm tra phiên bản hệ điều hành của thiết bị mạng để cập nhật, vá lỗi khi cần thiết. Sử dụng các công cụ để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng bảo mật và các trung cập bất hợp pháp vào hệ thống mạng. thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

c) Xác định và ghi rõ các tính năng an toàn, các mức độ bảo mật của dịch vụ và yêu cầu quản lý trong các thỏa thuận về dịch vụ mạng do bên thứ ba cung cấp.

d) Mạng không dây (Wi-Fi), thiết lập các thông số an toàn và định kỳ ít nhất 03 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn.

2. Cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố

a) Định kỳ hàng tháng hoặc khi có thay đổi cấu hình trên hệ thống, bộ phận chuyên trách thực hiện quy trình sao lưu dự phòng được sao lưu thông qua hệ thống sao lưu dữ liệu. Bản sao lưu được lưu trữ trên thiết bị hoặc hệ thống độc lập.

b) Các dữ liệu yêu cầu sao lưu, dự phòng gồm: Tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống theo yêu cầu của đơn vị vận hành.

c) Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

3. Truy cập và quản lý cấu hình hệ thống

a) Cán bộ quản lý, vận hành truy cập, khai thác thông tin theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

b) Cán bộ quản lý, vận hành có trách nhiệm theo dõi và phát hiện các trường hợp trung cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho Phòng Văn hóa – Xã hội để tiến hành ngăn chặn, thu hội, khóa quyền truy cập của các tài khoản vi phạm.

c) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

d) Quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy nhập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

4. Truy cập và quản lý cấu hình hệ thống

a) Cán bộ quản lý, vận hành truy cập, khai thác thông tin theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

b) Cán bộ quản lý, vận hành có trách nhiệm theo dõi và phát hiện các trường hợp trung cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho Bộ phận chuyên trách an toàn, an ninh mạng UBND xã Phước Giang để tiến hành ngăn chặn, thu hội, khóa quyền truy cập của các tài khoản vi phạm.

c) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

d) Quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy nhập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

Điều 13. Quản lý an toàn máy chủ và ứng dụng

1. Hệ thống thông tin phải được thiết kế thống nhất, được quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý và bảo đảm an toàn và bảo mật.

2. Hệ thống thông tin phải được bảo vệ bằng tường lửa và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng.

3. Mạng không dây (WI-FI), cần thiết lập các thông số an toàn và định kỳ ít nhất 03 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn.

4. Hoạt động của hệ thống phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của hệ thống.

5. Toàn bộ cấu hình hệ thống phải được sao lưu, dự phòng trên thiết bị hoặc hệ thống lưu trữ độc lập, định kỳ 01 tháng/lần.

6. Khi thực hiện nâng cấp, thay đổi cấu hình hệ thống phải thực hiện ngoài giờ làm việc.

7. Phải kiểm tra hoạt động tổng thể của hệ thống sau khi thay đổi cấu hình hoặc nâng cấp hệ thống.

8. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố:

a) Định kỳ hàng tháng hoặc khi có thay đổi, bộ phận chuyên trách thực hiện sao lưu, dự phòng hệ thống trên hệ thống độc lập như USB, DVD, SAN hoặc lưu trữ trên hạ tầng đám mây (cloud).

b) Các dữ liệu sau yêu cầu sao lưu, dự phòng: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

9. Truy cập và quản lý cấu hình hệ thống:

a) Cấu hình hệ thống từ xa phải sử dụng các giao thức bảo mật có mã hóa thông tin như SSL, TSL, SSH, VPN.

b) Khi cấu hình hệ thống từ bên ngoài phải thông qua kết nối VPN.

c) Toàn bộ cấu hình hệ thống phải được lưu trên thiết bị hoặc hệ thống lưu trữ độc lập.

Điều 14. Quản lý an toàn dữ liệu

1. Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn.

2. Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố ATTT mạng xảy ra.

3. Tiến hành cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ được thực hiện theo yêu cầu của đơn vị vận hành hệ thống.

4. Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ.

5. Quản lý chặt chẽ các thiết bị lưu trữ dữ liệu, nghiêm cấm việc di chuyển, thay đổi vị trí khi chưa được phép của người có thẩm quyền.

6. Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

7. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: Tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

8. Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ, phương tiện lưu trữ.

Điều 15. Quản lý sự cố an toàn thông tin

Chính sách, quy trình quản lý sự cố an toàn thông tin bao gồm:

- Có quy định về phân nhóm sự cố an toàn thông tin mạng

1. Phân nhóm sự cố an toàn thông tin mạng

Sự cố ATTT được phân loại theo hình thức bao gồm:

+ Sự cố do Tấn công từ chối dịch vụ

+ Sự cố do Mã độc, phần mềm độc hại

+ Sự cố do Truy cập trái phép

+ Sự cố do Vi phạm chính sách, Rò rỉ dữ liệu

+ Sự cố do Khai thác và thu thập thông tin trái phép (Hacking)

+ Sự cố do tấn công kỹ thuật

Mức độ sự cố phân loại theo mức độ ảnh hưởng và cấp độ hệ thống thông tin:

+ M1: Sự cố Nghiêm trọng

+ M2: Sự cố Lớn

+ M3: Sự cố Thông thường

Mức độ nghiêm trọng của sự cố ATTT được xác định trên cơ sở tổng hợp Cấp độ hệ thống và Mức độ ảnh hưởng theo bảng sau:

Mức độ ảnh hưởng	**Cấp độ hệ thống**				
	Cấp 1	**Cấp 2**	**Cấp 3**	**Cấp 4**	**Cấp 5**
Nghiêm trọng	**M3**	**M2**	**M1**	**M1**	**M1**
Lớn	**M3**	**M2**	**M2**	**M2**	**M1**
Thông thường	**M3**	**M3**	**M3**	**M2**	**M2**

2. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu và kế hoạch ứng phó sự cố an toàn thông tin mạng

- Ghi nhận, tiếp nhận thông báo, báo cáo sự cố an toàn thông tin mạng theo đúng quy trình.

- Thông báo ngay thông tin sự cố đến Phòng Văn hóa – Xã hội.

- Giám sát diễn biến tình hình ứng cứu sự cố và báo cáo Công an tỉnh; đề xuất, xin ý kiến chỉ đạo trong trường hợp không thuộc thẩm quyền, phạm vi trách nhiệm của mình hoặc vượt khả năng xử lý.

3. Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin

3.1 Phòng Tổng hợp chịu trách nhiệm:

a) Thực hiện theo dõi giám sát ATTT, ANM 24/7, tổng hợp thông tin dữ liệu;

b) Tổ chức, điều phối ứng cứu, xử lý, khắc phục khẩn cấp 24/7 các cuộc tấn công, sự cố ATTT, ANM;

3.2. Toàn thể các khoa, phòng chuyên môn và đơn vị chức năng trực thuộc, cùng với đội ngũ cán bộ, viên chức và người lao động đang công tác tại cơ quan trách nhiệm thông báo kịp thời tới Phòng Văn hóa – Xã hội hoặc cán bộ chịu

trách nhiệm ứng cứu và xử lý sự cố an toàn hệ thống thông tin khi gặp các sự kiện an toàn hệ thống thông tin bao gồm các tình huống sau:

a) Các lỗi, trục trặc trong hoạt động của phần mềm hoặc phần cứng;

b) Các tình huống vi phạm các quy định, quy tắc an toàn;

c) Các xâm nhập vào khu vực làm việc, khu vực an ninh trái phép;

d) Các thay đổi trên hệ thống không được cảnh báo hoặc lên kế hoạch;

đ) Các truy cập vào hệ thống trái phép;

e) Các tình huống bị lộ thông tin mức độ mật trở lên;

g) Các điểm yếu, lỗ hổng bảo mật trên các hệ thống thông tin có khả năng bị tấn công khai thác.

3.3. Cán bộ chịu trách nhiệm ứng cứu và xử lý sự cố an toàn hệ thống thông tin phải xem xét đánh giá các sự kiện an toàn hệ thống thông tin và xử lý khi thấy có thể xảy ra sự cố.

3.4. Hồ sơ xử lý sự cố

a) Quá trình xử lý sự cố phải được ghi chép và lưu trữ tại Ủy ban nhân dân xã.

b) Thu thập, ghi chép, bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố lặp lại trong tương lai. Trong trường hợp sự cố về thông tin có liên quan đến các vi phạm pháp luật, đơn vị có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền đúng theo quy định của pháp luật.

4. Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường

- Thực hiện cô lập hệ thống, ngắt kết nối với các hệ thống liên quan khác

- Khi có sự cố an toàn thông tin xảy ra, bộ phận chuyên trách phải sao lưu, dự phòng toàn bộ hiện trạng hệ thống trước khi xử lý sự cố

Thời gian khắc phục sự cố ATTT:

TT	Loại sự cố	Thời gian phản hồi	Mục tiêu phản hồi đúng thời hạn	Thời gian xử lý (khôi phục)	Mục tiêu khôi phục	Thời gian cập nhật thông tin xử lý
1	M3-Thông thường	60 phút	95%	03 ngày	98%	4 – 8 giờ/lần

5. Quy trình ứng cứu sự cố an toàn thông tin mạng lớn và nghiêm trọng

- Thực hiện cô lập hệ thống, ngắt kết nối với các hệ thống liên quan khác

- Khi có sự cố an toàn thông tin xảy ra, bộ phận chuyên trách phải sao lưu, dự phòng toàn bộ hiện trạng hệ thống trước khi xử lý sự cố

- Thông báo ngay cho Ban chỉ huy ứng cứu sự cố và lãnh đạo đơn vị để huy động nhân sự, phương tiện, và phối hợp các bộ phận liên quan. Liên hệ đơn vị chuyên trách hoặc cơ quan chức năng cấp trên (VD: VNCERT/CC) nếu cần hỗ trợ kỹ thuật hoặc điều phối quốc gia.

- Phân tích nguyên nhân, loại bỏ mã độc và lỗ hổng, khôi phục dữ liệu an toàn và giám sát hệ thống sau khi phục hồi.

Thời gian khắc phục sự cố ATTT:

TT	Loại sự cố	Thời gian phản hồi	Mục tiêu phản hồi đúng thời hạn	Thời gian xử lý (khôi phục)	Mục tiêu khôi phục	Thời gian cập nhật thông tin xử lý
1	M1-Nghiêm trọng	10 phút	99%	02 giờ	95%	30 phút/lần
2	M2-Lớn	30 phút	99%	08 giờ	98%	30 – 60 phút/lần

6. Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin: Phối hợp với Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao – Công an tỉnh và bên cung cấp dịch vụ thực hiện ứng cứu và khắc phục 24/7 với các sự cố mất ATTT ANM tại Ủy ban nhân dân xã.

Điều 16. Quản lý an toàn người sử dụng đầu cuối

1. Quản lý truy cập, sử dụng tài nguyên nội bộ

a) Người sử dụng khi truy cập, sử dụng tài nguyên phải tuân thủ các quy định của pháp luật về bảo đảm ATTT và các quy định của cơ quan, tổ chức.

b) Khi cài đặt, kết nối máy tính, thiết bị đầu cuối phải thực hiện theo hướng dẫn, quy trình dưới sự giám sát của bộ phận chuyên trách về ATTT.

c) Máy tính, thiết bị đầu cuối phải được xử lý điểm yếu ATTT, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

2. Quản lý truy cập, sử dụng tài nguyên trên Internet

a) Người dùng được quản lý và kiểm soát truy cập Internet thông qua firewall.

b) Các máy trạm đầu cuối được cài đặt phần mềm chống mã độc, cập nhật bản vá hệ điều hành và ứng dụng thường xuyên trước khi kết nối Internet.

c) Việc truy cập các dịch vụ đám mây, email cá nhân hoặc tải phần mềm từ Internet phải tuân thủ chính sách của đơn vị; các hành vi vi phạm sẽ bị ngăn chặn và xử lý.

d) Hoạt động truy cập Internet được lưu vết (log) và giám sát nhằm phát hiện sớm nguy cơ tấn công hoặc rò rỉ dữ liệu.

đ) Chỉ những người dùng được ủy quyền mới được phép sử dụng các dịch vụ công cộng qua Internet để trao đổi công việc.

3. Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:

a) Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB... phải thường xuyên quét virus trước khi đọc hoặc sao chép dữ liệu.

b) Không sử dụng các thiết bị máy tính cá nhân (như máy tính xách tay, thiết bị di động cá nhân, USB, ổ cứng di động...) vào mục đích công việc tại Đảng ủy, HĐND, UBND xã Phước Giang. Hạn chế tối đa việc sử dụng thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu liên quan đến chuyên môn, cán bộ nhân viên và các hoạt động của Đảng ủy, HĐND, UBND xã Phước Giang.

c) Các thiết bị đầu cuối khi kết nối phải được quản lý và cập nhật thông tin (tên, chủng loại, địa chỉ MAC, địa chỉ IP). Cần sử dụng cơ chế xác thực và sử dụng giao thức mạng an toàn

d) Bộ phận chuyên trách về an toàn thông tin phải thường xuyên theo dõi, kiểm tra các lỗ hổng bảo mật và quản lý kết nối, truy cập khi sử dụng thiết bị đầu cuối từ xa.

đ) Bộ phận chuyên trách về an toàn thông tin thường xuyên theo dõi cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống đối với các nhân viên đã nghỉ việc.

e) Bộ phận chuyên trách về an toàn thông tin thường xuyên theo dõi cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng.

Điều 17. Quản lý rủi ro an toàn thông tin mạng

Đơn vị vận hành xây dựng và ban hành Hồ sơ Quản lý rủi ro an toàn thông tin bao gồm các nội dung sau:

1. Danh mục tài sản thông tin, dữ liệu có trong hệ thống.

2. Đánh giá các rủi ro an toàn thông tin đối với mỗi loại tài sản.

3. Có phương án dự phòng và khôi phục sau sự cố đối với thông tin, dữ liệu và ứng dụng.

Điều 18. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Thực hiện hủy bỏ toàn bộ thông tin, dữ liệu trên hệ thống với sự xác nhận của đơn vị chủ quản HTTT khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ HTTT. Trong trường hợp thông tin, dữ liệu của HTTT lưu trữ trên tài sản vật lý, đơn vị chủ quản HTTT thực hiện các biện pháp tiêu hủy hoặc xóa thông tin bảo đảm không có khả năng phục hồi. Với trường hợp đặc biệt không thể tiêu hủy thông tin, dữ liệu thì sử dụng biện pháp tiêu hủy cấu trúc phần lưu trữ dữ liệu trên tài sản đó.

2. Đối với các HTTT có dữ liệu được lưu trữ trên tài sản vật lý cần phải mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài thì phải được sự phê duyệt của cấp có thẩm quyền và thực hiện các biện pháp bảo vệ dữ liệu; có cam kết bảo mật thông tin giữa bên có dữ liệu và bên cung cấp dịch vụ sửa chữa thiết bị lưu trữ dữ liệu.

Chương IV
KIỂM TRA, ĐÁNH GIÁ

Điều 19. Nội dung, hình thức kiểm tra, đánh giá

1. Nội dung kiểm tra, đánh giá:

a) Kiểm tra việc tuân thủ quy định của pháp luật và theo quy chế của Ủy ban nhân dân về bảo đảm an toàn HTTT theo cấp độ 2.

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn HTTT.

c) Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống.

d) Kiểm tra, đánh giá khác do chủ quản HTTT quy định.

2. Hình thức kiểm tra, đánh giá:

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của chủ quản HTTT.

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

3. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện nhiệm vụ kiểm tra, đánh giá.

4. Đối tượng kiểm tra, đánh giá là các đơn vị có HTTT hoặc đơn vị vận hành HTTT và các HTTT có liên quan.

Điều 20. Kiểm tra việc tuân thủ quy định về ATTT và hiệu quả của biện pháp bảo đảm ATTT

1. Nội dung kiểm tra, đánh giá

a) Kiểm tra việc xác định cấp độ an toàn HTTT và triển khai phương án bảo đảm ATTT; kiểm tra hiệu quả của các biện pháp bảo đảm ATTT.

b) Kiểm tra công tác giám sát ATTT; ứng cứu sự cố ATTT.

c) Kiểm tra các nội dung khác tại quy chế này.

2. Thẩm quyền kiểm tra

Văn phòng Uỷ ban nhân dân tỉnh Quảng Ngãi chịu trách nhiệm kiểm tra các đơn vị thuộc, trực thuộc Ủy ban nhân dân xã Phước Giang.

Chương V
TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 21. Trách nhiệm của UBND xã Phước Giang

Thực hiện trách nhiệm theo quy định tại Điều 22 Nghị định 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Điều 22. Trách nhiệm của Phòng Văn hóa – Xã hội

1. Giao Phòng Văn hóa – Xã hội xã Phước Giang là bộ phận chuyên trách về an toàn thông tin, có trách nhiệm bảo đảm an toàn thông tin cho hệ thống thông tin.

2. Tuân thủ các quy định về trách nhiệm của bộ phận chuyên trách về an toàn thông tin được giao tại Quy chế này.

Điều 23. Trách nhiệm của người dùng

Thực hiện nghiêm túc các quy định về quản lý, vận hành hệ thống tại đơn vị theo đúng các quy định hiện hành. Chấp hành đúng các quy định về bảo đảm an toàn thông tin trong quá trình sử dụng.

Chương VI
TỔ CHỨC THỰC HIỆN

Điều 24. Xây dựng và công bố

Quy chế này được tổ chức/bộ phận trình người đứng đầu đơn vị vận hành trước khi công bố áp dụng.

Điều 25. Trách nhiệm của UBND xã Phước Giang

1. Chủ trì, làm đầu mối hướng dẫn, theo dõi, giám sát, đôn đốc việc triển khai, tổ chức thực hiện Quy chế này.

2. Tiếp nhận và đưa ra các cảnh báo về an toàn, an ninh thông tin, áp dụng các biện pháp để khắc phục và hạn chế tối đa thiệt hại do sự cố mất an toàn, an ninh thông tin trong mạng Đảng ủy, HĐND, UBND xã.

3. Nhắc nhở, tạm dừng cung cấp các dịch vụ trong mạng Đảng ủy, HĐND, UBND, đối với đơn vị, người sử dụng có liên quan để kiểm tra, khắc phục sự cố. Trường hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục phải báo cáo Lãnh đạo xã và thông báo cho các tổ chức hỗ trợ xử lý sự cố mất ATTT để cùng phối hợp giải quyết.

4. Hàng năm, phối hợp với các đơn vị liên quan kiểm tra về công tác bảo đảm an toàn, an ninh thông tin mạng đối với các đơn vị thuộc, trực thuộc Đảng Ủy, HĐND, UBND.

5. Thực hiện việc cấp mới, chỉnh sửa, thu hồi tài khoản, mật khẩu, quyền truy cập và quyền khai thác tài nguyên mạng của Đảng ủy, HĐND, UBND cho người sử dụng khi có yêu cầu bằng văn bản.

6. Định kỳ hằng năm tiến hành rà soát Quy chế bảo đảm ATTT, an ninh mạng của UBND nhằm kiểm tra tính phù hợp, đồng thời cập nhật, chỉnh sửa và bổ sung khi cần thiết.

Điều 26. Trách nhiệm của các đơn vị thuộc và trực thuộc Đảng ủy, HĐND, UBND xã Phước Giang

1. Thủ trưởng các đơn vị thuộc, trực thuộc Đảng ủy, HĐND, UBND có trách nhiệm phổ biến, quán triệt đến toàn bộ công chức, viên chức, người lao động trong đơn vị thực hiện các quy định của Quy chế này.

2. Thủ trưởng các cơ quan, tổ chức, đơn vị có trách nhiệm tổ chức triển khai, chỉ đạo, kiểm tra và giám sát việc thực hiện các quy định về bảo đảm ATTT tại cơ quan, đơn vị thuộc phạm vi phụ trách; chịu trách nhiệm trước pháp luật và trước cấp có thẩm quyền nếu để xảy ra vi phạm trong lĩnh vực ATTT thuộc phạm vi quản lý.

3. Cung cấp thông tin người sử dụng của đơn vị khi có sự thay đổi để Phòng Văn hóa – Xã hội thực hiện cấp mới, sửa đổi, thu hồi thiết bị, tài khoản, mật khẩu truy cập và quyền khai thác tài nguyên mạng.

4. Bảo vệ, quản lý các trang thiết bị và tài nguyên mạng được lắp đặt tại đơn vị.

5. Chịu trách nhiệm về nội dung, thông tin truyền tải trong mạng theo quy định của pháp luật.

6. Trường hợp phát hiện sự cố mất an toàn, an ninh thông tin phải thông báo kịp thời tới Phòng Văn hóa – Xã hội bằng văn bản và các hình thức liên lạc khác để phối hợp giải quyết.

7. Tạo điều kiện thuận lợi cho Phòng Văn hóa – Xã hội và các đơn vị liên quan triển khai công tác kiểm tra, khắc phục sự cố khi xảy ra tình trạng mất an toàn, an ninh thông tin trong mạng Ủy ban nhân dân xã Phước Giang.

8. Phối hợp với cơ quan chức năng thẩm định về mặt kỹ thuật và công nghệ đối với các dự án, kế hoạch ứng dụng CNTT do đơn vị chủ trì.

9. Các đơn vị có HTTT có trách nhiệm đảm bảo ATTT mạng đối với HTTT của đơn vị mình quản lý và sử dụng; bố trí nhân sự để sẵn sàng xử lý sự cố ATTT mạng đối với các HTTT do đơn vị mình quản lý.

Điều 27. Kinh phí thực hiện

Kinh phí bảo đảm an toàn, an ninh thông tin mạng được lấy từ nguồn ngân sách nhà nước dự toán hàng năm của Uỷ ban nhân dân xã Phước Giang.

Điều 28. Khen thưởng, kỷ luật

1. Việc thực hiện đúng Quy chế này là một trong những tiêu chí bắt buộc để đánh giá kết quả công tác hằng năm của cá nhân và đơn vị, đồng thời là căn cứ xem xét thi đua, khen thưởng và xét tặng các danh hiệu đối với tổ chức, cá nhân.

2. Đơn vị, cá nhân vi phạm Quy chế này tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định của pháp luật.

Điều 29. Rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ 03 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.

2. Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng chính sách trong quá trình triển khai, áp dụng chính sách an toàn thông tin.

3. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh bằng văn bản về Bộ phận chuyên trách an toàn, an ninh mạng để tổng hợp, báo cáo Lãnh đạo xem xét điều chỉnh, bổ sung Quy chế cho phù hợp.